IN THE CLAIMS

1. (currently amended) A ~~distributed network security~~network system comprising:

a network~~, said network comprising~~configured to transport network traffic, wherein said network comprises a plurality of distributed security systems ~~and one or more networked systems of one or more types, said distributed security systems each comprising at least one host processor. a plurality of said distributed security systems~~ providing multiple protocol layer security ~~and comprising~~, wherein each of said distributed security systems comprises at least one host processor and said distributed security systems comprise a hardware processor offloading ~~or accelerating or sharply reducing~~ overhead of transport layer protocol processing from said at least one host processor ~~of said distributed security systems~~, wherein said hardware processor is other than said at least one host processor and is configured to receive a command from said at least one host processor,

said hardware processor comprising:

a protocol processing engine to do transport layer protocol ~~processing; or~~processing;

a programmable ~~rule processing~~rule-matching engine to analyze the network traffic for security rule matching or taking actions on matched ~~rules or a combination thereof; or~~security rules;

~~a security processing~~an authentication engine to do encryption, decryption, authorization or authentication ~~or a combination thereof~~ using standard or proprietary security ~~protocols; or~~protocols; and

a packet classification engine to classify the network traffic~~; or~~

~~a packet processing engine to perform packet processing tasks; or~~

~~a combination of any of the foregoing,~~

~~said distributed network security systems providing multiple protocol layer security in said network~~.

2. (currently amended) A security ~~system for~~system comprising:

a storage area network~~, said storage area network comprising one or more networked systems of one or more types~~configured to transport storage area network traffic, wherein said storage area network comprises at least one network system, ~~said security system comprising a set of systems from said one or more networked systems, a plurality of~~wherein said ~~set of systems comprising a.~~at least one network system comprises a hardware processor providing transport layer protocol processing,

said hardware processor comprising:

a storage protocol processing engine to do storage protocol ~~processing; or~~processing;

a protocol processing engine to do transport layer protocol ~~processing; or~~processing;

a programmable ~~rule processing~~rule-matching engine to analyze the storage area network traffic for security rule matching or taking actions on matched ~~rules or a combination thereof; or~~security rules;

~~a security processing~~an authentication engine to do encryption, decryption, authorization or authentication ~~or a combination thereof~~ using standard or proprietary security ~~protocols; or~~protocols;

a packet classification engine to classify the storage area network ~~traffic; or~~traffic; and

a packet processing engine to perform packet processing tasks like header processing or deep packet processing ~~or a combination thereof; or~~

~~a combination of any or the foregoing~~,

said security system providing multiple protocol layer security in said storage area network.

3. (currently amended) The ~~distributed network security~~network system of claim 1, further comprising:

a. at least one central manager for compiling and distributing security rules; and

b. at least one security policy driver to communicate with the central manager and to set up rules in said hardware processor ~~on at least one of said plurality of said one or more networked systems~~ to analyze and enforce security based on said rules.

4. (currently amended) The ~~distributed network security~~network system of claim 3, wherein said network comprises at least one network system, wherein the central manager comprises at least one of:

a. A Security Policy Developer Interface for entering security policy;

b. A Security Rules Compiler for compiling security policies into rules;

c. A Rules Distribution Engine to ~~distributed~~distribute rules to said ~~plurality of said one or more networked systems~~at least one network system;

d. A Security Policy Manager Interface to manage said ~~plurality of said one or more networked systems~~at least one network system;

e. A Security Monitoring Engine to monitor said network;

f. An event collection/management engine to manage said network and collect events or reports from at least one of said ~~plurality of said one or more networked systems~~at least one network system; or

g. a combination of any of the foregoing.

5. (currently amended) The ~~distributed network security~~network system of claim 3, wherein at least one of said distributed security systems ~~and networked systems~~ provides security based on rules for:

a. OSI protocol layer two to provide layer two or MAC layer filtering; or

b. OSI protocol layer three to provide layer three or network layer filtering; or

c. OSI protocol layer four to provide layer four or transport layer filtering; or

d. OSI protocol layers five through seven to provide upper layer or application layer filtering; or

e. a combination of any of the foregoing.

6. (currently amended) The ~~distributed network security~~network system of ~~claim 1 including security protocols comprising at least one of~~claim 1, further comprising at least one security protocol comprising IPSEC, OPSEC, SSL, TLS, AES, DES, 3DES, SHA1, MD4, MD5, RSA, CHAP, Kerberos, a proprietary protocol, or a combination of any of the foregoing.

7. (currently amended) The ~~distributed network security~~network system of claim 3, wherein at least one of the at least one policy drivers executes on ~~a processor of~~ said hardware processor ~~or on a~~or said at least one host processor ~~of at least one of said networked systems~~.

8. (currently amended) The ~~distributed network security~~network system of claim 1, said network system including multiple protocol layer security that includes security functions performed at one or more protocol layers of the OSI stack to provide packet filtering, intrusion detection, denial of service attack detection, port scanning detection, virus scan, spam filtering, unauthorized access, or a combination of any of the foregoing.

9. (currently amended) A security system comprising:

a network~~, said network comprising one or more networked systems of one or more types, a plurality of said one or more networked systems comprising~~configured to transport network traffic, wherein said network comprises a hardware processor providing a remote direct memory access ~~capability,~~(RDMA) capability and configured to offload transport layer protocol processing from a host processor that commands said hardware processor;

said hardware processor comprising:

an RDMA mechanism for performing RDMA data ~~transfer or~~transfer;

a protocol processing engine to do transport layer protocol ~~processing; or~~processing;

a programmable ~~rule processing~~rule-matching engine to analyze the network traffic for security rule matching or taking actions on matched security ~~rules or a combination thereof; or~~rules;

~~a security processing~~an authentication engine to do encryption, decryption, authorization or authentication ~~or a combination thereof~~ using standard or proprietary security ~~protocols; or~~protocols; and

a packet classification engine to classify the network traffic~~,; or~~

~~a packet processing engine to perform packet processing tasks like header processing or deep packet processing or a combination thereof; or~~

~~a combination of any of the foregoing.~~

said security system providing multiple protocol layer security in said network.

10. (canceled)

11. (currently amended) The security system of claim 9, further comprising:

a. at least one central manager for compiling and distributing security rules; and

b. at least one security policy driver to communicate with the central manager to set up rules in said hardware processor ~~on at least one of said plurality of said one or more networked systems~~ to analyze and enforce security based on said rules.

12. (currently amended) The security system of claim 11 wherein said network comprises at least one network system, and the central manager comprises at least one of:

a. A Security Policy Developer Interface for entering security policy;

b. A Security Rules Compiler for compiling security policies into rules;

c. A Rules Distribution Engine to distribute rules to said ~~plurality of said one or more networked systems~~at least one network system;

d. A Security Policy Manager Interface to manage said ~~plurality of said one or more networked systems~~at least one network system;

e. A Security Monitoring Engine to monitor said network;

f. An event collection/management engine to manage said network and collect events or reports from said ~~plurality of said one or more networked systems~~at least one network system; or

g. a combination of any of the foregoing.

13. (currently amended) The security system of claim 11 wherein said network comprises at least one ~~of said networked systems~~network system, said at least one network system provides security based on rules for

a. OSI protocol layer two to provide layer two or MAC layer filtering; or

b. OSI protocol layer three to provide layer three or network layer filtering; or

c. OSI protocol layer four to provide layer four or transport layer filtering; or

d. OSI protocol layers five through seven to provide upper layer or application layer filtering; or

e. a combination of any of the foregoing.

14. (currently amended) The security system of claim 9, ~~including security protocols~~further comprising at least one security protocol comprising ~~at least one of~~ IPSEC, OPSEC, SSL, TLS, AES, DES, 3DES, SHA1, MD4, MD5, RSA, CHAP, Kerberos, a proprietary protocol or a combination of any of the foregoing.

15. (currently amended) The security system of claim 11, wherein ~~at least one of~~ the at least one policy driver ~~that executes~~executes on ~~a processor of~~ said

hardware processor ~~or on a~~or on said host processor~~ of at least one of said networked systems~~.

16. (currently amended) The security system of ~~claim 9 including~~claim 9, wherein the multiple protocol layer security ~~that includes~~comprises a plurality of security functions performed at one or more protocol layers of ~~the OSI~~an OSI stack to provide packet filtering, intrusion detection, denial of service attack detection, port scanning detection, virus scan, spam filtering, unauthorized access, or a combination of any of the foregoing.

17. (currently amended) The ~~combination~~network system of claim 1 wherein said ~~one or more networked systems~~network comprises at least one network system, wherein said at least one networked system comprises a blade server, thin server, media server, streaming media server, appliance server, Unix server, Linux server, Windows or Windows derivative server, AIX server, clustered server, database server, grid computing server, VOIP server, wireless gateway server, security server, file server, network attached storage server, game server, router, switch, wireless access point, workstation, desktop computer, notebook computer, laptop computer, utility computing system or gateway device or a combination of any of the foregoing.

18. (currently amended) The ~~combination~~security system of claim 9 wherein said ~~one or more networked systems~~network comprises at least one network system, wherein said at least one network system comprises a blade server, thin server, media server, streaming media server, appliance server, Unix server, Linux server, Windows or Windows derivative server, AIX server, clustered server, database server, grid computing server, VOIP server, wireless gateway server, security server, file server, network attached storage server, game server, router, switch, wireless access point, workstation, desktop computer, notebook computer, laptop computer, utility computing system or gateway device or a combination of any of the foregoing.

19. (currently amended) The ~~distributed network security~~network system of claim 1, wherein said packet processing steps include header processing or deep packet processing or a combination thereof.

20. (currently amended) The security system of claim 2, further comprising:

a. at least one central manager for compiling and distributing storage area network security rules; and

b. at least one security policy driver to communicate with the central manager to set up rules in said hardware processor ~~on at least one of said plurality of said one or more networked systems~~ to analyze and enforce storage area network security based on said rules.

21. (currently amended) The security system of claim 20, wherein the central manager comprises at least one of:

a. A Security Policy Developer Interface for entering security policy;

b. A Security Rules Compiler for compiling security policies into rules;

c. A Rules Distribution Engine to distribute rules to the said ~~plurality of said one or more networked systems~~at least one network system;

d. A Security Policy Manager Interface to manage said ~~plurality of said one or more networked systems~~at least one network system;

e. A Security Monitoring Engine to monitor said network;

f. An event collection/management engine to manage said network and collect events or reports from said ~~plurality of said one or more networked systems~~at least one network system; or

g. a combination of any of the foregoing.

22. (currently amended) The security system of claim 20, wherein said at least one ~~of said networked systems~~network system provides security based on rules for

a. OSI protocol layer two to provide layer two or MAC layer filtering; or

b. OSI protocol layer three to provide layer three or network layer filtering; or

c. OSI protocol layer four to provide layer four or transport layer filtering; or

d. OSI protocol layers five through seven to provide upper layer or application layer filtering; or

e. Storage protocol layer to provide storage protocol layer filtering; or

f. a combination of any of the foregoing.

23 (currently amended) The security system of ~~claim 2 including security protocols~~claim 2, further comprising at least one security protocol comprising ~~at least one of~~ IPSEC, OPSEC, SSL, TLS, AES, DES, 3DES, SHA1, MD4, MD5, RSA, CHAP, Kerberos, a proprietary protocol or a combination of any of the foregoing.

24. (currently amended) The security system of ~~claim 20 including~~claim 20, further comprising a policy driver that executes on ~~a processor of~~ said hardware processor or on a host processor of ~~at least one of~~ said ~~networked systems~~at least one network system.

25. (currently amended) The security system of ~~claim 2 including~~claim 2, wherein the multiple protocol layer security ~~that includes~~comprises a plurality of security functions performed at one or more protocol layers ~~of the~~of an OSI stack to provide packet filtering, intrusion detection, denial of service attack detection, port scanning detection, virus scan, spam filtering, unauthorized access, or a combination of any of the foregoing.

26. (currently amended) A ~~distributed~~ network ~~security system for~~system comprising:

a network~~, said network comprising~~configured to transport network traffic, wherein said network comprises a plurality of distributed security systems ~~and one or more networked systems of one or more types, said distributed security systems comprising a set of systems from said one or more networked systems, and each comprising at least one host processor, a plurality of said set of systems~~ providing multiple protocol layer security, wherein each of said distributed security systems comprise at least one host processor and ~~comprising~~said distributed security systems comprise a hardware processor offloading ~~or accelerating or sharply reducing~~

overhead of transport layer protocol processing from said at least one host processor of said distributed security systems, wherein said hardware processor is other than said at least one host processor and is configured to receive a command from said at least one host processor;

said hardware processor comprising

a protocol processing engine to do transport layer protocol processing; or

a programmable ~~rule processing~~rule-matching engine to analyze the network traffic for security rule matching or taking actions on matched security rules ~~or a combination thereof~~; or

~~a security processing~~an authentication engine to do encryption, decryption, authorization or authentication ~~or a combination thereof~~ using standard or proprietary security protocols; or

a packet classification engine to classify the network traffic; or

a packet processing engine to perform packet processing tasks like header processing or deep packet processing or a combination thereof; or

a combination of the foregoing~~,~~

~~said distributed network security system providing multiple protocol layer security in said network~~.

27. (currently amended) A ~~distributed~~ network ~~security system for~~system comprising:

a network comprising a plurality of distributed security systems and one or more networked systems, each of said distributed security ~~systems each~~systems comprising at least one host processor, and at least one of said distributed security systems comprising a first hardware processor ~~offloading or accelerating or sharply reducing~~and a second hardware processor configured to offload overhead of a protocol processing stack from said at least one host processor ~~of said at least one of~~

~~said distributed security systems~~, said distributed ~~network~~ security systems providing a secure operating environment for said protocol processing stack for trusted computing needs of one or more of said networked systems by providing a policy driver for setting up the second hardware processor for a first set of security policy rules to be enforced by said second hardware processor, and a central manager for compiling and distributing said rules of the first set and monitoring the enforcement of said rules of the first set by said second hardware processor, wherein said central manager is configured to provide a second set of security policy rules to said first hardware processor, wherein the rules within the second set are different than the rules within the first set.

28. (currently amended) A ~~distributed~~ network ~~security~~ system comprising:

a network~~, said network~~ comprising a plurality of distributed security systems and one or more networked systems of one or more types, said distributed security systems ~~each comprising at least one host processor, a plurality of said distributed security systems~~ providing multiple protocol layer security ~~and comprising~~, wherein each of said distributed security systems comprise at least one host processor and said distributed security systems comprise a hardware processor offloading ~~or accelerating or sharply reducing~~ overhead of transport layer protocol processing from said at least one host processor ~~of said distributed security systems~~, wherein said hardware processor is other than said at least one host processor and is configured to receive a command from said at least one host processor, said hardware processor comprising a protocol processing engine to do transport layer protocol processing;

~~said distributed network security system providing multiple protocol layer security in said network~~.

29. (currently amended) The ~~hardware processor~~network system of claim 28, wherein said network transports network traffic, said hardware processor further comprising:

a programmable ~~rule processing~~rule-matching engine for analyzing the network traffic for security rule matching or taking actions on matched security rules ~~or a combination thereof~~;

~~a security processing~~an authentication engine for performing encryption, decryption, authorization or authentication ~~or a combination thereof~~ using standard or proprietary security protocols;

a packet classification engine to classify the network traffic; or

a packet processing engine to perform packet processing tasks; or

a combination of the foregoing,

30. (currently amended) The ~~hardware processor~~network system of claim 29, wherein said packet processing tasks comprise header processing, deep packet processing or a combination thereof.

31. (currently amended) A security ~~system for~~system comprising a storage area network~~, said storage area network comprising one or more networked systems of one or more types, said security system comprising a set of systems from said one or more networked systems, a plurality of said set of systems~~ comprising a hardware processor providing transport layer protocol processing, said hardware processor comprising a protocol processing engine for performing transport layer protocol processing; said security system providing multiple protocol layer security in said storage area network.

32. (currently amended) The ~~hardware processor~~security system of claim 31, wherein the storage area network is configured to transport storage area network traffic, said hardware processor further comprising:

a storage protocol processing engine for performing storage protocol processing;

a programmable ~~rule processing~~rule-matching engine for analyzing the storage area network traffic for security rule matching or taking actions on matched security rules ~~or a combination thereof~~;

~~a security processing~~an authentication ~~e~~engine for performing encryption, decryption, authorization or authentication ~~or a combination thereof~~ using standard or proprietary security protocols;

a packet classification engine for classifying the storage area network traffic; or

a packet processing engine for performing packet processing tasks; or

a combination of the foregoing.

33. (currently amended) The ~~distributed~~ network ~~security~~ system of claim 28, further comprising multiple protocol layer security that comprises security functions performed at one or more protocol layers of an OSI stack to provide packet filtering, intrusion detection, denial of service attack detection, port scanning detection, virus scan, spam filtering, unauthorized access, or detect other security attacks or a combination of any of the foregoing.

34. (currently amended) A security system comprising:

a network~~, said network comprising one or more networked systems of one or more types, a plurality of said one or more networked systems~~ comprising a hardware processor providing a remote direct memory access (RDMA) capability and configured to execute a transport layer protocol,

said hardware processor comprising an RDMA mechanism for performing RDMA data transfer, said security system providing multiple protocol layer security in said network.

35. (currently amended) The ~~hardware processor~~security system of claim 34 ~~further comprising~~, wherein said network is configured to transport network traffic, and said hardware processor further comprises:

a protocol processing engine for performing transport layer protocol processing;

a programmable ~~rule-processing~~rule-matching engine for analyzing the network traffic for security rule matching or taking actions on matched security rules ~~or a combination thereof~~; or

~~a security processing~~an authentication engine for performing encryption, decryption, authorization or authentication ~~or a combination thereof~~ using standard or proprietary security protocols;

a packet classification engine for classifying the network traffic; or

a packet processing engine for performing packet processing ~~tasks.~~tasks;

or a combination of the foregoing,

36. (currently amended) The ~~hardware processor~~security system of claim 35, wherein said packet processing comprises header processing, deep packet processing or a combination thereof.

37. (currently amended) The security system of ~~claim 34 where~~claim 34, wherein said hardware processor provides a transport layer remote direct memory access capability.

38. (currently amended) The security system of ~~claim 34 comprising~~claim 34, wherein the multiple protocol layer ~~security that~~security comprises a plurality of security functions performed at one or more protocol layers ~~of the~~of an OSI stack for providing packet filtering, intrusion detection, denial of service attack detection, port scanning detection, virus scan, spam filtering, unauthorized access, or detect other security attacks or a combination of any of the foregoing.

39. (currently amended) The ~~distributed network~~ security system of ~~claim 31 comprising~~claim 31, wherein the multiple protocol layer ~~security that~~security comprises a plurality of security functions performed at one or more protocol layers of the OSI stack for providing packet filtering, intrusion detection, denial of service attack detection, port scanning detection, virus scan, spam filtering, unauthorized access or a combination of any of the foregoing.

40. (currently amended) A security system comprising ~~a network, said network comprising one or more networked systems of one or more types, a plurality of said one or more networked systems comprising~~ a remote direct memory access (RDMA) ~~capability for performing~~processor configured to execute a plurality of RDMA data transfers and configured to execute a transport layer protocol,

said security system providing multiple protocol layer security in said network.

41. (currently amended) The ~~remote direct memory access capability~~security system of claim 40, further comprising a hardware processor~~, said hardware processor~~ comprising an RDMA mechanism for performing the RDMA data transfers.

42. (currently amended) The ~~remote direct memory access capability~~security system of claim 40, further comprising a hardware processor~~, said hardware processor~~ comprising a transport layer remote direct memory access capability.

43. (currently amended) The ~~hardware processor~~security system of claim 41 further comprising a hardware processor, said hardware processor comprising:

a protocol processing engine for performing transport layer protocol processing;

a programmable ~~rule processing~~rule-matching engine for analyzing network traffic for security rule matching or taking actions on matched security rules ~~or a combination thereof~~;

~~a security processing~~an authentication engine for performing encryption, decryption, authorization or authentication ~~or a combination thereof~~ using standard or proprietary security protocols;

a packet classification engine to classify the network traffic; or

a packet processing engine to perform packet processing ~~tasks.~~tasks; or

a combination of any of the foregoing.

44. (currently amended) The ~~hardware processor~~security system of claim 43, wherein said packet processing comprise header processing or deep packet processing or a combination thereof.

45. (currently amended) A security system comprising a storage area network~~, said storage area network comprising one or more networked systems of one or more types, a plurality of said one or more networked systems~~ comprising a remote direct memory access (RDMA) capability for performing RDMA data transfers, said security system providing multiple protocol layer security in said storage area network.

46. (currently amended) The ~~remote direct memory access capability~~security system of claim 45, further comprising a hardware processor~~, said hardware processor~~ comprising an RDMA mechanism for performing the RDMA data transfers.

47. (currently amended) The ~~remote direct memory access capability~~security system of claim 45, further comprising a hardware processor~~, said hardware processor~~ that provides a transport layer remote direct memory access capability.

48. (currently amended) ~~Said hardware~~The security system of claim 46, wherein said hardware processor ~~of claim 46~~ further ~~comprising~~comprises:

a storage protocol processing engine for performing protocol processing;

a protocol processing engine for performing transport layer protocol processing;

a programmable ~~rule processing~~rule-matching engine for analyzing storage area network traffic for security rule matching or taking actions on matched security rules ~~or a combination thereof~~;

~~a security processing~~an authentication engine for performing encryption, decryption, authorization or authentication ~~or a combination thereof~~ using standard or proprietary security protocols;

a packet classification engine to classify the storage area network traffic; or

a packet processing engine to perform packet processing ~~tasks.~~tasks; or

a combination of the foregoing.

49. (currently amended) The ~~hardware processor~~security system of claim 48, wherein said packet processing comprises header processing, deep packet processing or a combination thereof.

50. (currently amended) A ~~distributed~~ network ~~security~~ system comprising:

a network~~, said network comprising~~configured to transport network traffic, wherein said network comprises a plurality of distributed security systems ~~and one or more networked systems of one or more types, said distributed security systems each comprising~~providing multiple protocol layer security, wherein each of said distributed security systems comprise at least one host processor ~~a plurality of said distributed security systems providing multiple protocol layer security~~ and ~~comprising~~said distributed security systems comprise a hardware processor offloading ~~or accelerating or sharply reducing~~ overhead of transport layer protocol processing from said at least one host processor ~~of said distributed security systems~~, wherein said hardware processor is other than said at least one host processor and is configured to receive a command from said at least one host processor,

said hardware processor comprising:

a protocol processing engine to do transport layer protocol processing; and

a programmable ~~rule processing~~rule-matching engine for analyzing the network traffic for security rule matching or taking actions on matched security rules ~~or a combination thereof;~~

~~said distributed network security system providing multiple protocol layer security in said network~~.

51. (currently amended) A ~~distributed~~ network ~~security~~ system comprising:

a network~~, said network comprising~~configured to transport network traffic, wherein said network comprises a plurality of distributed security systems ~~and one or more networked systems of one or more types, said distributed security systems each comprising at least one host processor, a plurality of said distributed security systems~~ providing multiple protocol layer security ~~and comprising~~, wherein each of said distributed security systems comprise at least one host processor, and said distributed security systems comprise a hardware processor offloading ~~or accelerating or sharply reducing~~ overhead of transport layer protocol processing from said at least one host processor ~~of said distributed security systems~~, wherein said hardware processor is other than said at least one host processor and is configured to receive a command from said at least one host processor,

said hardware processor comprising:

a protocol processing engine for performing transport layer protocol processing;

a programmable ~~rule processing~~rule-matching engine for analyzing the network traffic for security rule matching or taking actions on matched security rules ~~or a combination thereof~~; and

~~a security processing~~an authentication engine to do encryption, decryption, authorization or authentication ~~or a combination thereof~~ using standard or proprietary security protocols~~;~~

~~said distributed network security system providing multiple protocol layer security in said network~~.

52. (currently amended) A security ~~system for a~~system comprising:

a storage area network~~, said storage area network comprising one or more networked systems of one or more types, said security system comprising a set of systems from said one or more networked systems, a plurality of said set of systems~~ comprising a hardware processor providing transport layer protocol processing, said hardware processor comprising ~~a protocol processing engine to do transport layer protocol processing; and~~ a storage protocol processing engine for performing storage protocol ~~processing;~~processing, said security system providing multiple protocol layer security in said storage area network.

53. (currently amended) The ~~hardware processor~~security system of claim 52, wherein said storage area network is configured to transport storage area network traffic, said hardware processor further comprising:

a programmable ~~rule processing~~rule-matching engine for analyzing the storage area network traffic for security rule matching or taking actions on matched security rules ~~or a combination thereof~~; or

~~a security processing~~an authentication engine for performing encryption, decryption, authorization or authentication ~~or a combination thereof~~ using standard or proprietary security protocols;

a packet classification engine for classifying the storage area network traffic; or

a packet processing engine for performing packet processing ~~tasks.~~tasks;

or a combination of any of the foregoing,

54. (currently amended) The ~~hardware processor~~security system of claim 53, wherein said packet processing comprises header processing or deep packet processing or a combination thereof.

55. (currently amended) A security system comprising:

a network~~, said network comprising one or more networked systems of one or more types, a plurality of said one or more networked systems~~ comprising a hardware processor providing a remote direct memory access (RDMA) capability,

said hardware processor comprising:

an RDMA mechanism for performing RDMA data transfer and

a protocol processing engine for performing transport layer protocol processing;

said security system providing multiple protocol layer security in said network.

56. (currently amended) The ~~hardware processor~~security system of claim 55, wherein said network is configured to transport network traffic, and said hardware processor further comprising:

a programmable ~~rule processing~~rule-matching engine for analyzing the network traffic for security rule matching or taking actions on matched security rules ~~or a combination thereof~~;

~~a security processing~~an authentication engine for performing encryption, decryption, authorization or authentication ~~or a combination thereof~~ using standard or proprietary security protocols;

a packet classification engine for classifying the network traffic; or

a packet processing engine to perform packet processing ~~tasks.~~tasks;

or a combination of the foregoing.

57. (currently amended) The ~~hardware processor~~security system of claim 56, wherein said packet processing ~~comprises.~~comprises header processing or deep packet processing or a combination thereof.

58. (currently amended) A security ~~system for~~system comprising:

a storage area network~~, said storage area network comprising one or more networked systems of one or more types, a plurality of said one or more networked systems~~ comprising a hardware processor providing a remote direct memory access (RDMA) capability,

said hardware processor comprising an RDMA mechanism for performing RDMA data transfer,

said security system providing multiple protocol layer security in said storage area network.

59. (currently amended) The ~~hardware processor~~security system of claim 58, wherein said storage area network is configured to transport network traffic, said hardware processor further comprising:

a storage protocol processing engine for performing storage protocol processing;

a protocol processing engine for performing transport layer protocol processing;

a programmable ~~rule processing~~rule-matching engine for analyzing the network traffic for security rule matching or taking actions on matched security rules ~~or a combination thereof~~;

~~a security processing~~an authentication engine to do encryption, decryption, authorization or authentication ~~or a combination thereof~~ using standard or proprietary security protocols; or

a packet classification engine to classify the network traffic; or

a packet processing engine to perform packet processing tasks; or

a combination of any of the foregoing.

60. (currently amended) The ~~hardware processor~~security system of claim 59, wherein said packet processing ~~comprises.~~comprises header processing or deep packet processing or a combination thereof.

61. (currently amended) The ~~hardware processor~~security system of claim 32, wherein said packet processing tasks comprises header processing or deep packet processing or a combination thereof.

62. (currently amended) A ~~multiple protocol layer distributed~~ network ~~security~~ system ~~for a network~~comprising a network further comprising a plurality of distributed security systems and ~~one or more networked systems~~at least one network system, wherein each of said distributed security systems ~~each comprising~~comprises at least one host processor ~~at least one of said distributed security systems having~~and said distributed security systems comprise a hardware processor offloading ~~or accelerating or sharply reducing~~ overhead of at least one of a transport layer protocol processing stack and a network layer protocol processing stack from said at least one host processor ~~of said at least one of said distributed security systems~~, wherein said hardware processor is other than said at least one host processor and is configured to receive a command from said at least one host processor, said distributed ~~network~~ security systems providing a secure operating environment for said protocol processing stack for trusted computing needs of ~~one or more of said networked systems~~said at least one network system ~~using~~and said distributed network security systems providing multiple protocol layer security in said network.

63. (new) A network system in accordance with Claim 1, wherein said hardware processor is configured to analyze the network traffic communicated at a rate of at least one of 1 Gigabits per second and 10 Gigabits per second.

64. (new) A security system in accordance with claim 2, wherein said storage area network is configured to implement a Small Computer System Interface over Internet (iSCSI) protocol.